REMARKS

In the Official Action mailed on **31 May 2006,** the Examiner reviewed claims 1, 4, 7-12, 15, 18-23, 26 and 29-33. Claims 1, 4, 7-12, 15, 18-23, 26, and 29-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dickinson et al (USPN 6,853,988, hereinafter "Dickinson").

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 12, and 23 were rejected as being unpatentable over Dickinson. Examiner avers that Dickenson discloses "the implementation of user identifier or user identification and an application identifier, which identifies what type of algorithm to be used to sign the message" (see Office Action, page 6, point 2). The cited passage discusses identifying which algorithm type was used to generate a certificate for the user (see Dickenson column 21, lines 25-40). This is not the same as identifying an **application being used**. Identifying which algorithm type was used generate the certificate for the user does not address the problem of preventing a user who has access to a first application, but who does not have access to a second application, from gaining access to the second application.

Applicant reiterates that the present invention receives **a user identifier and an application identifier** (see page 9, lines 20-21 of the instant application), and looks up a key pair based on **a user identifier and an application identifier** (see page 10, lines 9-14 of the instant application). The present invention then uses the identified private key to sign a form on behalf of the user (see page 10, lines 15-16 of the instant application). This is beneficial because it allows the signature server to sign a document on behalf of a user *only if* the user is allowed to sign for a given application. Hence, even if the user has a valid key pair for other applications, the signature server will not sign on behalf of the user unless the user is authorized to sign for the given application.

There is nothing within Dickinson, either explicit or implicit, which suggests receiving a user identifier and an application identifier at a signature server, and looking up a private key for the user based on the user identifier and the application identifier, wherein looking up a private key for the user based on the user identifier and application identifier prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used.

Accordingly, Applicant has amended independent claims 1, 12, and 23 to clarify that the present invention looks up a private key for the user at the signature server based on the user identifier and the application identifier, *wherein looking up a private key for the user based on the user identifier and application identifier prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used.* These amendments find support in on page 9, lines 20-21, and page 10, lines 9-14 of the instant application.

Hence, Applicant respectfully submits that independent claims 1, 12, and 23 as presently amended are in condition for allowance. Applicant also submits that claims 4 and 7-11, which depend upon claim 1, claims 15 and 18-22, which depend upon claim 12, and claims 26 and 29-33, which depend upon claim 23, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By _____

Edward J. Grundler
Registration No. 47,615

Date: 21 June 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
edward@parklegal.com